The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

03/11/2014

SUBJECT:

Vulnerability in Microsoft Silverlight Could Allow For Security Feature Bypass (MS14-014)

EXECUTIVE SUMMARY:

A vulnerability has been discovered in the Microsoft Silverlight which could allow an attacker to take complete control of an affected system. Microsoft Silverlight is a web application framework that provides support for .NET applications and used for streaming media. The vulnerabilities can be exploited if a user visits or is redirected to a malicious web page, or runs a specially crafted Silverlight application.

Successful exploitation could result in an attacker gaining the ability to exploit vulnerabilities that were previously protected. In other words, an attacker could tie this security feature bypass vulnerability to an additional vulnerability, most likely a remote code execution vulnerability. These vulnerabilities could then allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

At this time these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Microsoft Silverlight 5
- Microsoft Silverlight 5 Developer Runtime

RISK:

Government:

- Large and medium government entities: **High**

- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Asecurity feature bypass vulnerability has been discovered in Microsoft Silverlight due to improper implementation of Data Execution Protection (DEP) and Address Space Layout Randomization (ASLR).

An attacker could exploit this vulnerability by creating a web site that contains a specially crafted Silverlight content designed to exploit this vulnerability. The security feature bypass by itself does not allow arbitrary code execution. However, successful exploitation could result in an attacker gaining the ability to exploit vulnerabilities that were previously protected by DEP and ASLR. In other words, an attacker could tie this security feature bypass vulnerability to an additional vulnerability, most likely a remote code execution vulnerability. These vulnerabilities could then allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

By default, Internet Explorer on Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 runs in a restricted mode that is known as Enhanced Security Configuration. This mode mitigates this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Microsoft immediately after appropriate testing.
- If there is no business need, then consider disabling Microsoft Silverlight.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Microsoft:

https://technet.microsoft.com/en-us/security/bulletin/ms13-087

https://technet.microsoft.com/en-us/security/bulletin/ms14-014

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0319